State of Maryland

State of Maryland

Department of Budget and Management

Statewide Security Support

Introduction to the State of Maryland IT Security Certification and Accreditation Guidelines

October 31, 2002

Prepared By:
Mark Jenkins, Senior Engineer/Analyst

Science Applications International Corporation
An Employee-Owned Company
Science Applications International Corporation
13921 Park Center Road, Suite 300
Herndon, VA 20171

Abridged from SAIC-6099-2002-122

Prepared For:
Carmella Thompson, Assistant Director of Security
Department of Budget and Management, Office of Information Technology
45 Calvert Street
Annapolis, MD 21401

RECORD OF CHANGES

This Page Intentionally Left Blank

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABRIDGED FROM SAIC-6099-2002-122
OCTOBER 31, 2002

Introduction to the State of Maryland IT Security Certification and Accreditation Guidelines

EXECUTIVE SUMMARY

The IT Security C&A process evaluates the implementation of an IT system or site against its security requirements. The process produces evidence used by a designated manager as part of the basis for making an informed decision about operating that IT system or site. The process is implemented by a C&A team comprised of individuals filling four key roles: Designated Accrediting Authority (DAA), Certifier, Program Manager, and Business Operations Representative. Throughout the process, work done by the C&A team is recorded in a single document, the System Security Consensus Document (SSCD). At the critical accreditation decision point, the SSCD represents the material evidence supporting the system C&A recommendation. Following accreditation, this document is maintained in order to represent the security posture of the system.

The checklist in Table Exec-1 represents a summary of the tasks to be accomplished within the certification and accreditation process, divided by process phase and activity. These tasks are executed within the development lifecycle for developing systems. When certifying and accrediting an existing system, this list represents a rough ordering of the tasks. In both cases, parallel activity is both feasible and normally desirable for the greatest efficiency.

The C&A tasks are identified using the convention of an abbreviation for the phase of the C&A process where the task is performed and a number for the sequence of the task in that phase. For example, Task Ver-1 refers to a task conducted in Phase 2, Verification, of the C&A process; and the task is the first conducted during Phase 2.

Table Exec-1: C&A Task Checklist

Activity	√	Task Description	Task ID
Phase 1: Definition			
Preparation		Review Documentation	Def-1
Registration		Prepare Mission Description and System Identification	Def-2
		Inform the C&A Team (Register the System)	Def-3
		Prepare the Environment and Threat Description	Def-4
		Determine the System Security Requirements	Def-5
		Prepare the System Architecture Description	Def-6
		Identify the C&A Organizations and the Resources Required	Def-7
		Tailor the C&A Process and plan work	Def-8
		Draft the SSCD	Def-9
Negotiation		Review Draft SSCD	Def-10
		Conduct Certification Requirements Review	Def-11
		Establish Consensus on Level of Effort and Schedule	Def-12
		Approve Phase 1 SSCD	Def-13
Decision Point: Consensus for Phase 1 SSCD?			

Activity	√	Task Description	Task ID
Phase 2: Verification			
Systems Development and Integration		Review SSCD	Ver-1
Initial Certification Analysis		Analyze System Architecture	Ver-2
		Analyze Software, Hardware, and Firmware Design	Ver-3
		Analyze Network Connection Rule Compliance	Ver-4
		Analyze Integrity of Integrated Products	Ver-5
		Analyze Life Cycle Management	Ver-6
		Prepare Security Requirements Validation Procedures	Ver-7
		Evaluate Vulnerabilities	Ver-8
Decision Point: Sufficient Compliance to Proceed?			
Phase 3: Validation			
Certification Evaluation of Integrated System		Review SSCD	Val-1
		Test and Evaluate Security Controls	Val-2
		Test Penetration Resistance	Val-3
		Analyze System Management	Val-4
		Evaluate Site	Val-5
		Evaluate Contingency Plan	Val-6
		Review Risk Management	Val-7
Decision Point: System Meets Requirements?			
Develop Recommendation		Complete Accreditation Package	Val-8
Decision Point: System Accreditation?			
Phase 4: Post-Accreditation			
System Operations/ Security Operations		Maintain SSCD	PA-1
		Review Physical, Personnel, and Management Controls	PA-2
		Maintain Contingency Plan	PA-3
		Manage Configuration	PA-4
		Manage System Security	PA-5
		Review Risk Management	PA-6
Decision Point: Validate Compliance?			
Validate Compliance		Validation tasks as appropriate	PA-7-n
Decision Point: Recertify and Reaccredit?			

1. INTRODUCTION

1.1. Background

Developing and operating Information Technology (IT) systems is a partnership between business (also known as functional) staff and IT specialists. The overall responsibility of each State of Maryland Executive Branch Agency (or Department) is protecting the systems and the information stored, processed, and communicated through those systems from inappropriate, unplanned, and unlawful disclosure, modification, destruction, or loss of availability. As such, the protection of information is a part of the partnership between the business staff and the IT specialists. A key aspect of the relationship is providing assurance that the systems and information are appropriately protected. The certification and accreditation process is a mechanism for creating that assurance.

> Certification – The comprehensive assessment of the technical and non-technical security features and other safeguards of a system to establish the extent to which a particular system meets a set of specified security requirements for its use and environment.
>
> Accreditation – Formal declaration by a Designated Approval Authority (DAA) that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

State policy for IT systems requires that all Executive Branch agencies certify and accredit the IT systems and sites under their ownership and control. The Department of Budget and Management (DBM) is responsible, under Maryland State Law, for developing, maintaining, revising, and enforcing information technology policies and standards. These guidelines were developed under that authority.

The State of Maryland chose to include a security Certification and Accreditation (C&A) process as part of the IT lifecycle for state government systems. IT Security C&A programs are required of federal government departments and agencies, and a significant amount of knowledge and expertise has been amassed by the federal government with respect to programs and processes of this nature. The Maryland C&A programs and processes have been derived from a common body of knowledge surrounding the federal programs and processes, adapted for use within the State's environment.

1.2. Purpose

The purpose of these guidelines is to establish a documented IT security C&A process for the State of Maryland Executive Branch of government. This C&A process is part of the risk management process for IT systems and sites. The C&A process provides assurance that the security risk to the systems and sites certified and accredited was determined to be at a level acceptable to those managers.

These guidelines enhance the risk management process for IT systems and sites. The programs and methods included provide a formal mechanism for evaluating: how well IT systems meet information security requirements; the level of risk that remains; and, whether or not to operate those systems at that level of risk. Implementing these guidelines, as part of the practice of acquiring and operating IT systems, will ensure that these issues are given due consideration throughout the process and provide an increased level of security awareness throughout an organization. The following objectives accomplish this purpose:

- Provide a procedure for performing security certification and accreditation activities for IT systems and sites at the agency level,
- Show how the IT security certification and accreditation procedure is integrated into the Systems Development Lifecycle and IT Investment Management processes,
- Identify the roles and responsibilities for security certification and accreditation activities, and map those roles and responsibilities to typical State of Maryland Executive Branch agency positions, and
- Describe the basic outline of security certification and accreditation programs to be implemented at the agency and state levels in order to put these guidelines into practice.

1.3. Scope

These guidelines apply to all agencies of the Executive Branch of the government of the State of Maryland. Each IT system and site operated by or on behalf of these agencies (including those operated by contractors) is to be evaluated and accredited using the guidelines, as part of a C&A program that meets these requirements.

1.4. Policy/Authorization

The Maryland Code, Law Pertaining to Information Processing, State Finance and Procurement, Title 3, Subtitle 4, 3-401 to 3-413 authorizes these guidelines. Section 3-403 (a) charges the Secretary of the DBM with responsibility “for developing, maintaining, revising, and enforcing information technology policies and standards.” Section 3-410 authorizes the Chief of Information Technology (also known as the State CIO) to carry out certain duties for the Secretary of the DBM. Section 3-410 (d) (1) charges the Chief to be responsible to the Secretary of the DBM for carrying out the duty of “developing, maintaining, and enforcing statewide information technology standards, policies, and procedures.” The State CIO has created the Security and Architecture Division within the Office of Information Technology of the Department of Budget and Management to assist the State CIO. The Deputy Director for Security of the Security and Architecture Division commissioned these guidelines.

1.5. Change Process

The Assistant Director for Security (ADS) is responsible for maintaining this guideline document and ensuring version control. A scheduled review will occur at least annually. The ADS is responsible for scheduling this review and informing participants. In addition, the ADS will ensure this document is reviewed for impact when there are modifications to state security policies.

Changes to this document will be recorded on the Record of Changes Page immediately following the Table of Contents. The ADS is responsible for distributing the revisions to the Agency CIO's for distribution to appropriate staff and for maintaining the master copy of the document.

1.6. Assumptions

The following assumptions were made during the preparation of this document:

- This Introduction will be used only to supplement and not to replace the Guidelines

1.7. Roles and Responsibilities

Head of Agency

- Implements C&A Program at agency level, and
- Assigns Designated Approving Authorities (DAAs) to systems and sites.

Program Manager

- Represents the interests of the system throughout its lifecycle,
- Coordinates all aspects of the system from initial concept through development, implementation, operations and maintenance, to disposal,
- Ensures that security requirements are integrated in a way that results in an acceptable level of risk to the operational infrastructure as determined via the C&A process,
- Keeps all C&A process participants informed of lifecycle actions, documented user needs, and security requirements, and
- Usually initiates the C&A process.

Note: As a system passes through different phases of the life cycle, the assignment of this role will pass from a development organization to an operations organization and finally to a maintenance organization.

Designated Approving Authority (DAA)

- The primary government official responsible for implementing system security,
- Has authority and ability to evaluate mission, business case, and budgetary needs for the system in view of security risks,
- Determines acceptable level of residual risk for systems and sites,
- Accepts (accredits) or rejects the current level of risk for the operation of a system and site,
- Directs the security activities of the Certifier and Information System Security Officer or other systems security staff, and
- Provides advice, information, and guidance to the Program Manager.

Note: The more sensitive the system, the more senior the DAA(s) should be.

Certification Authority (Certifier)

- Provides technical expertise to conduct the certification through the system life cycle,
- Determines the level of residual risk, identifies notable risk details, and makes accreditation recommendation to the DAA, and
- Provides advice, information, and guidance to the Program Manager.

Note: The Certifier should be independent from the development/operation of the system.

Business Operations Representative

- Represents the operational interests of the system's users,
- Ensures that the business' operational interests are maintained throughout the system's lifecycle,
- Acts as liaison for the business operations community during the life cycle of the system,
- During C&A, is concerned with system availability, access, integrity, confidentiality, functionality, and performance as they relate to the business mission environment, and
- Provides advice, information, and guidance to the Program Manager.

Information Systems Security Officer (ISSO)/Security Staff

- Monitors the secure operation of the system and site by the business operations community, and
- Ensures the system and site is deployed and operated according to the documented security requirements through integration of all security disciplines (Management, Operational, and Technical) to maintain an acceptable level of risk.

2. UNDERSTANDING YOUR ROLE IN THE C&A PROCESS

The five sections that follow provide a personal perspective on the Certification and Accreditation Process for the Head of Agency role and the four key C&A Team roles: Designated Approving Authority, Program Manager, Certifier, and Business Operations Representative. These sections supplement the role and responsibility descriptions provided in Section 1.7, *Roles and Responsibilities*.

Of the four C&A Team roles, only the Certifier has a unique existence in the C&A process. The other three roles, although named within the C&A process, are filled by people with primary responsibilities outside of the C&A process.

Table 2-1: Alignment of C&A Team Roles with Existing Agency Roles

C&A Role	Primary Role Outside of C&A
Designated Approving Authority	Senior manager with authority and responsibility over one or aspects of the business, system, or data
Program Manager	System development manager or system operations manager, depending on the life cycle stage of the system
Certifier	None
Business Operations Representative	Manager within the business operations community

2.1. Head of Agency

As the Head of Agency, you are responsible for ensuring that a Certification and Accreditation Program is implemented within your Agency. The program should be compliant with the guidelines issued by the Department of Budget and Management, Office of Information Technology, Security and Architecture Division. The State of Maryland IT Security Certification and Accreditation Guidelines have specific recommendations on establishing Agency-level C&A programs.

In addition to making sure that a C&A program is established within your Agency, you are also responsible for designating who has the authority to approve the operation of each of the IT systems within your Agency. The individuals you select for each system are known as the Designated Approving Authorities for that system.

2.2. Designated Approving Authority

As the Designated Approving Authority for a system going through the Certification and Accreditation process, you are expected to work with the other Certification and Accreditation roles (Program Manager, Certifier, and Business Operations Representative) as a Team to achieve a consensus on the security for the system to be certified and accredited. You may be acting alone in your role, or as part of a team of DAAs. You were selected for this role because of your position of authority over and responsibility for an aspect of the system that is being certified and accredited. This aspect may be the business operations supported by the system, the IT operations that will run the system to support the business operations, or responsibility for the data that is processed, stored, or transmitted by the system.

Within the C&A process, your role has the ultimate responsibility of approving or disapproving the operation of the system; approving the operation is referred to as "accrediting the system." Your decision will be based in part on the evaluation and certification of the system performed by or under the direction of the Certifier role. The Certifier will provide you with information regarding how well the system meets its security requirements, and what the residual risks are in operating the system. If these residual risks are acceptable to you in context with all of the other constraints upon your organization and responsibilities, then you accredit the system. If they are not, then you disapprove the operation of the system. In some cases the risks may not be completely acceptable to you, but the system may still need to be put into operation before all of the unacceptable risks can be mitigated. In this case, you may issue an "interim authority to operate", or IATO. The IATO permits operation of the system under the condition that the unacceptable risks are mitigated according to a strategy and schedule acceptable to you. This mitigation plan is developed by you and the other Certification and Accreditation Team roles.

You should be familiar with the general nature of the Certification and Accreditation process, but you are not expected to be expert in its particulars. The Certifier will provide detailed explanations of any aspect of the process for which you require clarification as you perform your duties. The Program Manager or the Certifier will be responsible for the majority of the work products. You must participate in decision making processes as the work progresses.

You should be familiar with the high-level business and security considerations for the elements of the organization for which you are responsible. The Business Operations Representative will handle the business operations details. The Program Manager will handle the technical details.

2.3. Program Manager

As the Program Manager for a system for a system going through the Certification and Accreditation process, you are expected to work with the other Certification and Accreditation roles (Designated Approving Authority, Certifier, and Business Operations Representative) as a Team to achieve a consensus on the security for the system to be certified and accredited. You were selected for this role because of your responsibility for the development or operation of the system (depending on where the system is in its life cycle).

Within the C&A process, you are responsible for organizing, scheduling, and determining the funding for the Certification and Accreditation activities, and integrating them into the development or operations of the system being processed within the general constraints established through consensus with the other C&A Team members. In some cases, the Certifier may handle many of these details, especially for an independent certification of an existing system. You also have a primary responsibility for ensuring that the security requirements for the system are defined, although you should expect assistance from the other C&A Team members with all aspects of your role.

You should be moderately familiar with the Certification and Accreditation process in general, and with the work products and scheduling requirements in particular. The Certifier will provide detailed explanations of any aspects of the process for which you require clarification as you perform your duties. The DAA role will be responsible for establishing high-level directions with respect to cost, security, and business functionality.

Within your development or operations processes, you are responsible for the implementation of the security requirements for which a consensus has been reached among the C&A Team, and the integration of the security controls that implement these requirements with all other aspects of the system. The Business Operations Representative will represent the needs of the business operations user community to you as you carry out your responsibilities. The quality of the system development or operation, within the high-level constraints established by the DAA role and the more immediate business concerns of the Business Operations Representative, is in your hands.

2.4. Certifier

As the Certifier for a system for a system going through the Certification and Accreditation process, you are expected to work with the other Certification and Accreditation roles (Designated Approving Authority, Program Manager, and Business Operations Representative) as a Team to achieve a consensus on the security for the system to be certified and accredited. You were selected for this role because of your knowledge and skills in the area of IT security certification and accreditation, and that is your primary focus area.

Within the C&A process, you are responsible for performing the Verification (Phase 2) and Validation (Phase 3) activities with support from the other C&A Team members and providing a recommendation to the DAA with respect to accrediting the system. You are generally regarded as the expert on the C&A process, and will provide detailed explanations of the process to other C&A Team members when requested. In some cases, you may also be responsible for some of the Program Manager's responsibilities, such as organizing, scheduling, and determining the funding requirements for the Certification and Accreditation activities, especially if you are handling an independent certification of an existing system.

2.5. Business Operations Representative

As the Business Operations Representative for a system going through the Certification and Accreditation process, you are expected to work with the other Certification and Accreditation roles (Designated Approving Authority, Program Manager, and Certifier) as a Team to achieve a consensus on the security for the system to be certified and accredited. You were selected for this role because of your ability to represent the needs of the business operations community supported by the system.

Within the C&A process, you are responsible for representing the needs of the business operations community, and for establishing the security rules of behavior for users of the system.

You should be generally familiar with the Certification and Accreditation process, and with the purpose and use of the security rules of behavior in particular. The Certifier will provide detailed explanations of any aspects of the process for which you require clarification as you perform your duties.

You should also represent your business operations community's needs within the development or operations processes for the system. You should have some role in establishing the processes and procedures to enforce the security rules of behavior for users of the system.

3. CERTIFICATION AND ACCREDITATION PROCESS SYNOPSIS

The C&A process is designed to provide a standardized set of engineering, evaluation, and documentation activities leading to a successful system accreditation and secure system operation. Standardizing these activities helps ensure a consistent application of the process and interpretation of the process results from system to system. Consistent application and interpretation is especially important when systems are interconnected or utilize a shared infrastructure.

The key actors in the C&A process are a group of four individual roles: the Program Manager, the DAA, the Certifier, and the Business Operations Representative. The people that fill these roles are called the C&A Team. The actual number of individuals involved depends on the size, complexity, and sensitivity of the system and the requirements of the agency's C&A program.

The C&A process can be applied to systems in different circumstances. It can be used within a lifecycle model for a new system under development or an evolving system undergoing significant change. It can also be applied to an existing system to assess its security posture for the first time, or as part of a recurring activity that assesses the system periodically in order to maintain its security posture. The process includes a tailoring step to customize the tasks to the manner in which the process is being applied (new system and site, evolving system and site, existing unchanged system and site) as well as to the particulars of the system or site, including the sensitivity and criticality of the system or site.

Each phase and activity of the C&A process must be performed, but the tasks in each activity are tailored and scaled to the manner of application, the system, and its associated acceptable level of residual risk. The implementation of the C&A process is expected to be tailored and integrated with on-going systems acquisition activities to best fit the mission, environment, system architecture, and programmatic considerations. This tailoring is a significant part of the work done by the C&A team in Phase 1.

Throughout the process, a single document, entitled the System Security Consensus Document (SSCD), is used to record the results of the certification and accreditation work. This document then contains the foundation for the accreditation decision that takes place prior to placing the system into operation or being permitted to continue to operate. Following the accreditation of a system, the SSCD is kept up-to-date and represents the expected security posture of the system.

A high-level pictorial representation of the C&A process flow is depicted in Figure 3-1.

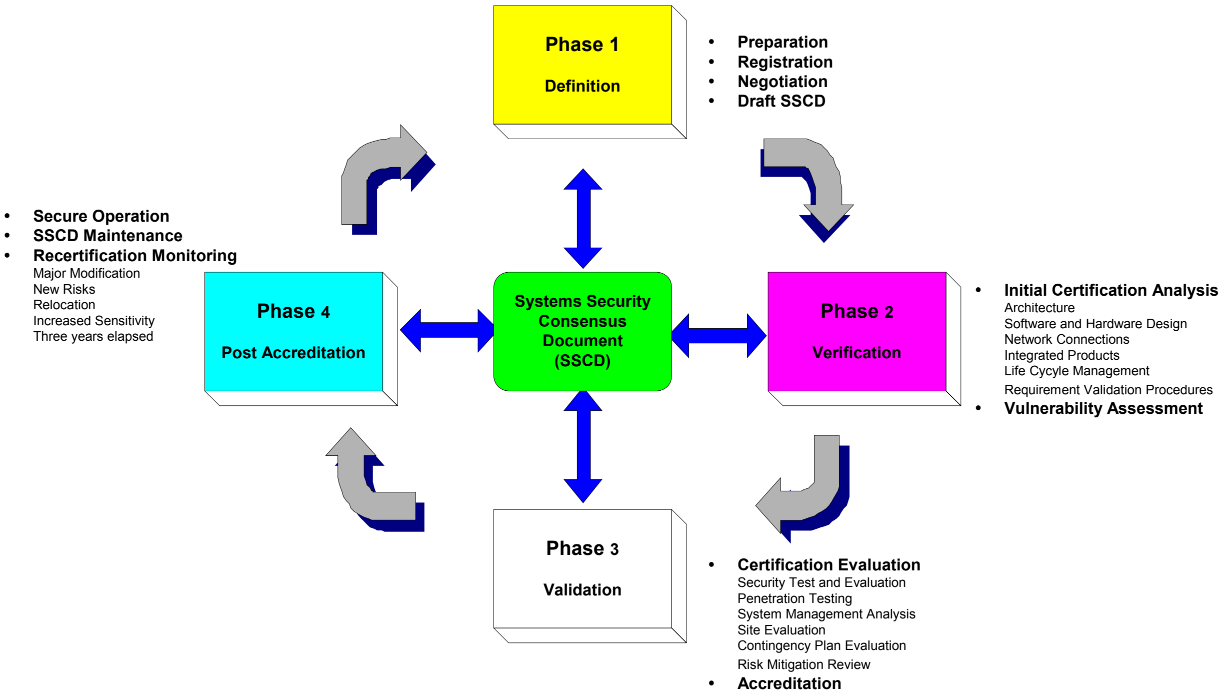

Figure 3-1: C&A Process Overview

3.1. C&A Phases

The C&A process is divided into four ordered phases as shown in Figure 3-1; Definition, Verification, Validation, and Post Accreditation. Each phase has a particular focus, consistent with a generalized system lifecycle model. Every C&A effort starts with Phase 1 and progresses through subsequent phases in order. A system is likely to cycle through the C&A process more than once during its operational lifetime. When the process is applied to an existing system rather than one under development, the four phases are still used. The emphasis within the phases shifts, however, from an interactive relationship between the C&A process and the developmental process to a one-way information flow from the existing system documentation into the C&A process.

Phase 1: Definition focuses on understanding the IS business case, environment, and architecture to determine the security requirements and level of effort necessary to achieve certification and accreditation. The objective of Phase 1 is to agree on the security requirements, C&A boundary, schedule, level of effort, and resources required.

Phase 2: Verification confirms the evolving or modified system's compliance with the information in the SSCD. The objective of Phase 2 is to ensure the fully integrated system will be ready for certification testing.

Phase 3: Validation corroborates compliance of the fully integrated system with the security policy and requirements stated in the SSCD. The objective of Phase 3 is to produce the required evidence to support the DAA in making an informed decision to grant approval to operate the system (accreditation or Interim Approval to Operate (IATO)).

Phase 4: Post Accreditation starts after the system has been certified and accredited for operations. Phase 4 includes those activities necessary for the continuing operation of the accredited system in its computing environment and to address the changing threats and small-scale changes a system faces through its life cycle. The objective of Phase 4 is to ensure secure system management, operation, and maintenance to preserve an acceptable level of residual risk.

The process cycles back to Phase 1 when a situation requiring re-certification occurs. These situations include a major system modification, discovery of new risks, relocation to a new environment, or increased system sensitivity or criticality. In the absence of any other factor, the process cycles back to Phase 1 for re-certification and re-accreditation at periodic intervals based on a schedule determined by the C&A team and/or the agency's C&A program.

3.2. C&A Process Features

Several features of the C&A Methodology are critical for understanding and carrying out the process. They are:

- Accreditation Boundary
- Single C&A Document
- C&A Consensus
- LifeCycle Integration and Tailoring
- Certification Levels
- Continuous Security Assurance

Each of these is described in more detail below.

3.2.1. C&A Boundary

A key registration task (the Registration activity is in the Definition Phase) is to prepare a description of the accreditation boundary (system boundary, facilities, equipment, etc.) and the external interfaces with other equipment or systems. The accreditation boundary includes all information system equipment that is to be addressed in the C&A. Therefore, the information system facilities and equipment must be under the control of the DAA. Any interconnected facility or equipment that is not included or is not under the control of the DAA is considered as an external interface.

3.2.2. Single C&A Document

A single document approach is used in the C&A process. All the information relevant to the C&A is collected into one document, the SSCD depicted in the center of Figure 3-1 above. The SSCD was designed to meet all the requirements for C&A support documentation.

The SSCD is a documented statement of consensus among the members of the C&A team. The SSCD is used throughout the entire C&A process to guide actions, document decisions, specify information assurance requirements, document certification tailoring and level of effort, identify possible solutions, and maintain operational systems security. The characteristics of an SSCD are listed in Table 3-1 below.

Table 3-1: SSCD Characteristics

1.	Describes the operating environment and threat.
2.	Describes the system security architecture.
3.	Establishes the C&A boundary of the system to be accredited.
4.	Documents the consensus among the DAA(s), certifier, program manager, and Business Operations Representative.
5.	Documents all requirements necessary for accreditation.
6.	Documents all security criteria for use throughout the information system life cycle.
7.	Minimizes documentation requirements by consolidating applicable information into the SSCD (security policy, concept of operations, architecture description, etc.).
8.	Documents the C&A plan.
9.	Documents test plans and procedures, certification results, and residual risk.
10.	Forms the baseline security configuration document.

For Type accreditations, an SSCD may be prepared for the system software and hardware considered under the type accreditation. This SSCD is shipped to each prospective installation site with the software and hardware and included by reference in the SSCD for each of the actual implementations of the system design that received the Type accreditation. After installation of the information system, the information from the type SSCD is included in the target system's (network or site) SSCD. The system configuration and security environment must still be certified during Phase 3 to ensure it meets the specifications found in the SSCD for the Type accreditation. See Section 3.4, C&A Accreditation Objects, for more information about Type accreditations.

3.2.3. C&A Consensus

The key to a successful accreditation and secure operation is the consensus between the members of the C&A team, represented by the roles of DAA, certifier, program manager, and Business Operations Representative. These individuals resolve critical schedule, budget, security, functionality, and performance issues. This consensus is documented in the SSCD. The SSCD is used to guide and document the results of the C&A process. The objective is to use the SSCD to establish an evolving, yet authoritative, consensus on the level of security required for C&A. After accreditation, the SSCD becomes the baseline security configuration document.

3.2.4. Life Cycle Integration and Tailoring

The C&A process applies to all systems requiring accreditation throughout their life cycle. It is designed to be adaptable to any type of information system, any computing environment, and any mission. It may be adapted to include existing system certifications, evaluated products, new security technology or programs, and any set of applicable standards. The C&A process may be mapped to any system life cycle process but is independent of the life cycle strategy. The process is designed to adjust to the development, modification, and operational life cycle phases. The implementation details of C&A process activities may be tailored and, where applicable, integrated with other acquisition and documentation activities. Tailoring information is found throughout the task descriptions and in Section 5.1, Adjusting the C&A Process to a Particular C&A Effort.

Details on how the C&A process maps to a particular lifecycle methodology, the State of Maryland SDLC, are contained in the *State of Maryland IT Security Certification and Accreditation Guidelines*, Section 6, Relationship with other Lifecycle Management Processes. This particular lifecycle methodology is also assumed as the standard throughout the descriptions of the C&A process wherever process elements related to a lifecycle methodology are presented.

3.2.5. Certification Levels

The C&A process has four levels of certification to provide the flexibility for appropriate assurance within schedule and budget limitations. The difference between the levels is the depth of the analysis applied. Certification Level 1 is a basic security review, Level 2 is a minimum analysis, Level 3 is a detailed analysis, and Level 4 is a comprehensive analysis. To determine the appropriate level, the certifier analyzes the system business functions, State of Maryland, State department or agency security requirements, criticality of the system to the agency mission including the impact of a failure on Maryland citizens, software products, computer infrastructure, data processed by the system, and types of users. Considering this information, the certifier determines the degree of assurance required for the confidentiality, integrity, availability, and accountability controls of the system. Further information regarding Certification Levels can be found in the *State of Maryland IT Security Certification and Accreditation Guidelines*, Table 4-4 under the description of Task Def-8, Tailor the C&A Process and Plan Work.

The selected certification level is used to guide the level effort involved in the C&A process. The C&A process descriptions provide task-level details for tailoring the level of effort to the desired certification level.

More information on selecting a certification level is found in the *State of Maryland IT Security Certification and Accreditation Guidelines*, Section 5.3, Critical Task and Procedure Details.

3.3. Continuous Security Assurance

In recognition of the fact that systems undergo a variety of changes to the system itself and to the environment within which the system operates, the C&A process provides for three levels of maintenance of the security posture created when a system is accredited. By cycling through each of the three levels, a continuous assurance of security is approximated. The three levels, from the smallest in scope and effort to the largest, are:

- System and Security Operations Activity in the Post Accreditation Phase – small-scale, standard operating procedures that continuously monitor, manage, and maintain the elements of the security environment for the system.
- Compliance Validation Activity in the Post Accreditation Phase – a medium-scale, periodic activity that re-examines some aspects of the security posture and serves as a catalyst for updating elements if necessary.
- Recertification and Reaccreditation – a large-scale, periodic or conditionally initiated activity that analyzes the entire system and its security to determine if security requirements are still being met and residual risk is being maintained at a level acceptable to the DAA.

The timing of the Compliance Validation Activity cycle and the timing and conditions for the Recertification and Reaccreditation cycle is determined by the C&A Team and documented in the SSCD as part of the C&A process tailoring task. Minimum requirements for timing and conditions are available to the C&A team from the Agency or Statewide C&A Program.

3.4. C&A Accreditation Objects

The C&A process has three categories of accreditation objects. They are:

- Systems
- Sites
- Types

The C&A process is substantially the same for each of these categories. Different areas of emphasis may exist, and are highlighted in the C&A tailoring task undertaken by the C&A Team in the Definition Phase.

Systems. An information system processes, stores, and/or transmits information. The systems category is further subdivided into General Support Systems (GSS) and Non-minor Applications.[1] GSS are platforms supporting multiple applications, such as a mainframe computing system, an interactive timesharing system, a LAN server and its clients, or a communications network (either Local Area or Wide Area). A Minor Application is one that derives most, if not all, of its security from the General Support System upon which it runs, making it unnecessary to conduct a C&A against it. A Non-minor Application is any other

[1] NIST documentation and US federal government agency documents and processes generally use the term "major application" where this C&A process description uses "non-minor application." The use of the term "major application" has been avoided due to the prior definition and use of the term "major information technology development project" in State of Maryland legislation. The manner in which major is used is more restrictive than is intended by these guidelines, and so the use of the term "major application" has been avoided in favor of "non-minor application." Note that any system identified as a "major application" following the definition from Maryland law would quality as a "Non-minor Application" under these guidelines.

Application. Examples of Non-Minor Applications include: payroll systems, personnel systems, and web portals. Systems are selected for accreditation based on a high-level risk assessment, usually conducted as part of a C&A Program. A GSS accreditation, if available, is used to support (reduce the workload for) a Non-minor Application accreditation.

Note: The designation "Non-minor Application" is applied broadly to any system significant enough to require accreditation that is not a GSS. The use of the word "application" should not be construed as limiting the designation to software applications alone. Standalone hardware/software systems, including associated network components that are not part of a GSS, are designated "Non-minor Applications."

Sites. A site is a physical location encompassing IT operations, such as a data center or an office containing IT workers. Sites are selected for accreditation based on a high-level risk assessment, usually conducted as part of a C&A Program. It is not necessary for a site to have a separate accreditation; each system to be accredited at a site can include all of the site considerations. However, a Site accreditation, if available, is used to support (reduce the workload for) the accreditation of the Systems operating at that site.

Types. In some situations, a common set of software, hardware, and firmware is installed at multiple locations. Since it is difficult to accredit the common systems at all possible locations, a type accreditation may be created for a typical operating environment. The type accreditation is the official authorization to employ identical copies of a system in a specified environment. The type system SSCD must include a statement of residual risk and clearly define the intended operating environment. The SSCD must also identify specific uses of the system, operational constraints, and procedures under which the type system may operate. The program manager, Business Operations Representative, and ISSO ensure that the proper security operating procedures, configuration guidance, and training is delivered with the system.

Accreditation testing of each implementation is limited to confirming that the original configuration and security posture has been reproduced.

Examples of situations where a type accreditation would be used include establishing a standard Windows workstation operating system configuration, establishing requirements for deploying Blackberry hand-held e-mail devices, establishing a standard LAN deployment template, etc.

3.5. Ancillary Material

The appendices of the guidelines, when coupled with the body of the guideline, include all of the instructions and information necessary for accomplishing the C&A of a system, site, or type.

3.6. C&A Road Map

The C&A process road map in Figure 3-2 below shows the progression of a system through the four C&A phases. The C&A process begins with the accumulation of Phase 1 inputs shown in the top left corner of Figure 3-2. The system then progresses through the Phase 1 activities of preparation, registration, and negotiation shown as boxes in the figure. During these activities, the associated tasks listed below the respective boxes in the figure are completed. In like manner, the figure shows the system progression through Phase 2, Verification, and Phase 3, Validation. The Validation phase culminates in the accreditation of the system. Finally, progression of the system into Phase 4, Post Accreditation activities is shown. The system remains in Phase 4 until a recertification monitoring condition triggers initiation of a new system C&A. The system then reenters Phase 1 of the C&A processes at the encircled "A" entry point shown in the figure.

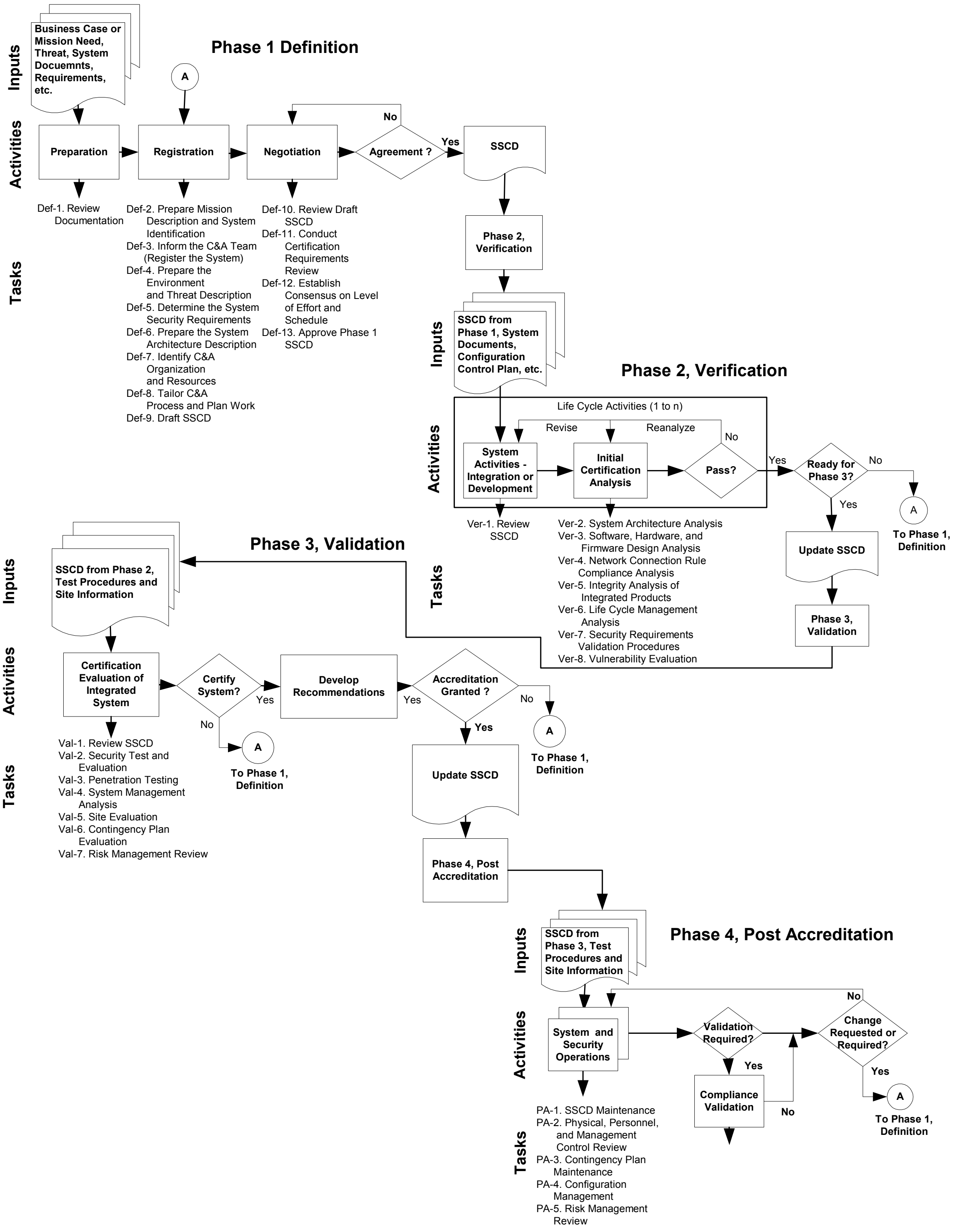
Phase 1 Definition
Inputs
Business Case or Mission Need, Threat, System Docuemnts, Requirements, etc.
A
Activities
Preparation
Registration
Negotiation
Agreement ?
No
Yes
SSCD
Tasks
Def-1. Review Documentation
Def-2. Prepare Mission Description and System Identification
Def-3. Inform the C&A Team (Register the System)
Def-4. Prepare the Environment and Threat Description
Def-5. Determine the System Security Requirements
Def-6. Prepare the System Architecture Description
Def-7. Identify C&A Organization and Resources
Def-8. Tailor C&A Process and Plan Work
Def-9. Draft SSCD
Def-10. Review Draft SSCD
Def-11. Conduct Certification Requirements Review
Def-12. Establish Consensus on Level of Effort and Schedule
Def-13. Approve Phase 1 SSCD
Phase 2, Verification
Phase 2, Verification
Inputs
SSCD from Phase 1, System Documents, Configuration Control Plan, etc.
Activities
Life Cycle Activities (1 to n)
Revise
Reanalyze
No
System Activities - Integration or Development
Initial Certification Analysis
Pass?
Yes
Ready for Phase 3?
No
Yes
A
To Phase 1, Definition
Tasks
Ver-1. Review SSCD
Ver-2. System Architecture Analysis
Ver-3. Software, Hardware, and Firmware Design Analysis
Ver-4. Network Connection Rule Compliance Analysis
Ver-5. Integrity Analysis of Integrated Products
Ver-6. Life Cycle Management Analysis
Ver-7. Security Requirements Validation Procedures
Ver-8. Vulnerability Evaluation
Update SSCD
Phase 3, Validation
Phase 3, Validation
Inputs
SSCD from Phase 2, Test Procedures and Site Information
Activities
Certification Evaluation of Integrated System
Certify System?
Yes
No
A
To Phase 1, Definition
Develop Recommendations
Yes
Accreditation Granted ?
No
A
To Phase 1, Definition
Yes
Update SSCD
Phase 4, Post Accreditation
Tasks
Val-1. Review SSCD
Val-2. Security Test and Evaluation
Val-3. Penetration Testing
Val-4. System Management Analysis
Val-5. Site Evaluation
Val-6. Contingency Plan Evaluation
Val-7. Risk Management Review
Phase 4, Post Accreditation
Inputs
SSCD from Phase 3, Test Procedures and Site Information
Activities
System and Security Operations
Validation Required?
Yes
Compliance Validation
No
Change Requested or Required?
No
Yes
A
To Phase 1, Definition
Tasks
PA-1. SSCD Maintenance
PA-2. Physical, Personnel, and Management Control Review
PA-3. Contingency Plan Maintenance
PA-4. Configuration Management
PA-5. Risk Management Review

Figure 3-2: C&A Process Flow Chart

3.7. Roles and Responsibilities by Phase

3.7.1. Phase 1 Roles and Responsibilities

Table 3-2 shows the C&A process responsibilities assigned to each role during Phase 1 Activities and Tasks.

Table 3-2: Phase 1 Key Role Responsibilities

Phase	Management Roles	Security Roles		Business Operations Roles
	Program Manager	**DAA**	**Certifier**	**Business Operations Representative**
Phase 1	Initiate security dialogue with DAA, certifier, and Business Operations Representative Define system schedule and budget, including C&A process Support C&A process tailoring and level of effort determination Define system architecture Prepare Life Cycle Management Plans Define security architecture	Define accreditation requirements Obtain threat assessment Assign the certifier Support C&A process tailoring Approve the SSCD	Begin vulnerability and risk assessments Review threat definition Lead C&A process tailoring Determine level of certification effort Describe certification team roles and responsibilities Draft SSCD	Support C&A process tailoring and level of effort determination Define operational needs in terms of mission Identify vulnerabilities to mission Define operational resource constraints

3.7.2. Phase 2 Roles and Responsibilities

Table 3-3 shows the C&A process responsibilities assigned to each role during Phase 2 Activities and Tasks.

Table 3-3: Phase 2 Key Role Responsibilities

Phase	Management Roles	Security Roles		Business Operations Roles
	Program Manager	DAA	Certifier	Business Operations Representative
Phase 2	Develop system or develop system modification Word contractual and service level agreements with external entities in a manner that ensures compliance with these guidelines Support certification activities Review certification results Revise system as needed Resolve security discrepancies	Support certification activities	Conduct certification activities Assess vulnerabilities Report results to the program manager, DAA, and Business Operations Representative Determine if system is ready for certification Update the SSCD	Prepare security Rules of Behavior (ROB) and Security Operating Procedures (SOP) Support certification actions

3.7.2.1. ISSO Responsibilities

During Phase 2, the ISSO is responsible for the tasks shown in Table 3-4.

Table 3-4: Phase 2 ISSO Responsibilities

1.	Review the mission statement to determine if it accurately describes the system.
2.	Review the environment description to determine if it accurately describes the system.

3.7.3. Phase 3 Roles and Responsibilities

Table 3-5 shows the C&A process responsibilities assigned to each role during Phase 3 Activities and Tasks.

Table 3-5: Phase 3 Key Role Responsibilities

Phase	Management Roles	Security Roles		User Roles
	Program Manager	DAA	Certifier	Business Operations Representative
Phase 3	Support certification activities Provide information system access for ST&E Provide system corrections under configuration management	Assess vulnerabilities and residual risk Decide to accredit, issue an Interim Authority to Operate, or terminate system operations	Conduct certification activities Evaluate security requirements compliance Assess vulnerabilities and residual risk Report results to the program manager, DAA, and Business Operations Representative Recommend risk mitigation measures Prepare final SSCD Recommend accreditation type	Support certification efforts Implement and maintain Security Operating Procedures (SOP) and Rules Of Behavior (ROB) Review certification results

3.7.4. Phase 4 Roles and Responsibilities

Table 3-6 shows the C&A process responsibilities assigned to each role during Phase 4 Activities and Tasks.

Table 3-6: Phase 4 Key Role Responsibilities

Phase	Management Roles	Security Roles		User Roles
	Program Manager	DAA	Certifier	Business Operations Representative
Phase 4	Update information system to address Phase 3 reported vulnerabilities and patches under configuration management Report security related changes to the information system to the DAA and Business Operations Representative Review and update life cycle management policies and standards Resolve security discrepancies	Review the SSCD Review proposed changes Oversee compliance validation Monitor C&A integrity Decide to reaccredit, accredit, issue an IATO, or; if SSCD is no longer valid, terminate system operations		Report vulnerability and security incidents Report threats to mission environment Review and update system vulnerabilities Review and change security policy and standards Initiate SSCD review if changes to threat or system

3.7.4.1. ISSO Responsibilities

The ISSO is usually the security focal point within the user community, responsible for the secure operation of the information system within the environment agreed on in the SSCD. The ISSO ensures the information system is deployed and operated according to the SSCD through integration of all the security disciplines (technical, management, and operational controls) to maintain an acceptable level of residual risk. The responsibilities of the ISSO during Phase 4 include those shown in Table 3-7.

Table 3-7: Phase 4 ISSO Responsibilities

1.	Periodically review the mission statement, operating environment, and security architecture to determine compliance with the approved SSCD.
2.	Maintain the integrity of the site environment and accredited security posture.
3.	Ensure that configuration management adheres to the security policy and security requirements.
4.	Initiate the C&A process when periodic reaccredidation is required or system change dictates.